

REMARKS

The foregoing Amendment and the following Remarks are submitted in response to the Office Action issued on April 26, 2005 in connection with the above-identified patent application, and are being filed within the three-month shortened statutory period set for a response by the Office Action.

Claims 1-9, 11-14, 16-32, 34-37, and 39-46 remain pending in the present application, and stand rejected. Independent claim 1 has been amended to include the subject matter of claims 10 and 15, and independent claim 24 has likewise been amended to include the subject matter of claims 33 and 38. Accordingly, claims 10, 15, 33, and 38 have been canceled and depending claims 11, 16, 18-20, 34, 39, and 41-43 have been amended to adjust dependencies. Applicants respectfully submit that no new matter has been added to the application by the Amendment.

The Examiner has rejected claims 1-46 under 35 USC § 103 as being obvious over Minear et al. (U.S. Patent No. 5,983,350) in view of Douglas (U.S. Patent Application Pub. No. 2004/0010684). Applicants respectfully traverse the § 103 rejection of such claims.

Independent claim 1 recites a method for releasing digital content to a rendering application, where the rendering application forwards the digital content to an ultimate destination by way of a path therebetween. Significantly, the path is defined by at least one module and the digital content is initially in an encrypted form.

In the method, an authentication of at least a portion of the path is performed to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough. If in fact each such defining module is to be trusted based on the authentication, the encrypted digital content is decrypted and forwarded to the

rendering application for further forwarding to the ultimate destination by way of the authenticated path.

As amended, independent claim 1 also recites that in performing the authentication, at least a portion of the path is traversed to develop a map of each module in the path, and each module in the map is authenticated. Also, for each module in the at least a portion of the path, such authentication includes receiving from the module a certificate as issued by a certifying authority, and determining from the received certificate whether such received certificate is acceptable for purposes of authenticating the module.

Independent claim 24 as amended recites substantially the same subject matter as claim 1 as amended, albeit as a computer-readable medium having computer-executable instructions thereon that perform the method.

To review, with the present invention, encrypted content is decrypted and released to a rendering application only after an authentication determines that trust may be imparted to the path that the rendering application will employ to forward the decrypted content to the ultimate destination. Among other thing, then, then, the present invention requires –

- (1) a rendering application forwarding digital content to an ultimate destination by way of a path therebetween, where the path is defined by at least one module;
- (2) an authentication of the path by way of authenticating each module in a map developed of the path, where such authentication includes receiving and reviewing a certificate from each module; and
- (3) a decryption and forwarding of decrypted content through the path, but only if the authentication succeeds.

The rendering application may be any application that renders content, such as an audio player rendering audio from audio content, a video player rendering video from video content, a visual renderer rendering a picture from picture content, or the like. Significantly, the path is not merely a wire or a communications channel, but is defined by interconnected modules, such as for example audio filters, video filters, picture filters, and the like. Also significantly, each module may be represented in a map of the path, and each module can provide a certificate to authenticate same.

As was previously pointed out, inasmuch as the content passing through the modules / filters that define the path is to be decrypted content, such modules / filters of the path must be trusted to handle the decrypted content in a trusted manner, and are therefore each authenticated to determine trustworthiness. Such trust is for example with regard to the fact that the modules / filters defining the path will not copy the decrypted content for nefarious purposes.

In the course of being authenticated, a particular module proves its trustworthiness by proffering a digital certificate issued by a certifying authority. Thus, with the present invention a path of such modules may be trusted to transit decrypted content to an ultimate destination without allowing such content to be diverted to a nefarious entity.

The Minear reference discloses a method and mechanism by which a message is received over the Internet, particularly where the message has been encrypted by the sender according to a particular IPSEC standard. As best set forth at column 5, line 34 through column 6, line 26, the message is received over an unprotected network 16 by a firewall 18 of a workstation 20 and accordingly is in the encrypted form. As the message passes through a network protocol stack 40 of the workstation 20, it is determined that the message is

encrypted and therefore such message is decrypted (column 6, lines 9-13) and forwarded through the stack 40 for further processing, including authentication of the sender (column 6, lines 13-18). The Minear reference also speaks of authenticating sent packets (column 3, lines 64-66) and authenticated communications session between a sending and receiving firewall (column 4, lines 37-42).

Significantly, although the Minear reference speaks of authenticating in at least the three instances set forth above, such Minear reference is entirely silent regarding any authentication of the path through which the decrypted message flows. Accordingly, the Minear reference does not at all disclose authenticating a path through which decrypted content is forwarded, as is required by claims 1 and 24. As may be appreciated, in the Minear reference such path would include that part of the stack 40 after the message has been decrypted. As may also be appreciated, such path would not include the Internet inasmuch as the Minear message within such Internet is disclosed as being encrypted.

Moreover, and at any rate, the Minear reference clearly discloses that the decrypting of the message takes place before authentication of same. Accordingly, such Minear reference cannot be said to disclose a decryption and forwarding of decrypted content through a path, but only if an authentication (performed prior to such decryption) succeeds, as is also required by claims 1 and 24. As should be understood, it makes little sense to decrypt content to be sent down an exposed path if the path is not first authenticated, especially if a failure of the path to authenticate would obviate the need for such decryption.

At any rate, the Examiner admits that the Minear reference does not teach authenticating at least a portion of a path to determine whether each module therein can be

trusted. Nevertheless, the Examiner argues that the Douglas reference teaches such an authentication.

The Douglas reference in point of fact discloses a method of exchanging objects over an insecure network. In the method, and as may best be seen in connection with Fig. 8, clients A and B in the course of sequentially sending each other objects each maintain a count. When one of A or B sends an object to the other, such A or B includes in the sent object an incremented count maintained by A and an incremented count maintained by B, as well as a signature over the contents of the sent object, a certificate for validating the signature, and one or more keys, presumably in connection with the certificate. Thus, each sent object as received is validated based on the incremented counts, the keys, the certificate, and the signature thereof.

Thus, the sent objects as set forth in the Douglas reference are themselves authenticated based on the information therein as being from a particular source (A or B). Significantly, though, such sent objects are not disclosed as being digital content sent from a rendering application to an ultimate destination by way of a path therebetween, where the path is defined by at least one module, as is required by claims 1 and 24. Instead, such Douglas sender and receiver are each computers, the path is a networking arrangement between the computers, and such path is not disclosed as being defined by modules.

In addition, the Douglas reference does not disclose or suggest an authentication of the path by way of authenticating each module in a map developed of the path, where such authentication includes receiving and reviewing a certificate from each module, as is required by claims 1 and 24. Instead, the Douglas reference only discloses authenticating the sent objects and not the path through which such objects transit, does not

employ a map developed of the modules of the path, and does not receive and review certificates from any such modules.

Finally, the Douglas reference does not disclose or suggest a decryption and forwarding of decrypted content through a path, but only if the authentication succeeds, as is required by claims 1 and 24. Instead, the Douglas sender sends an object via the network arrangement and the sent object is authenticated after being received.

To conclude then, neither the Minear reference nor the Douglas reference, alone or combined, discloses:

- (1) a rendering application forwarding digital content to an ultimate destination by way of a path therebetween, where the path is defined by at least one module;
- (2) an authentication of the path by way of authenticating each module in a map developed of the path, where such authentication includes receiving and reviewing a certificate from each module; and
- (3) a decryption and forwarding of decrypted content through the path, but only if the authentication succeeds.

Thus, for the aforementioned reasons, Applicants respectfully submit that the Minear and Douglas references cannot be combined to make obvious the subject matter recited in claims 1 or 24, or any claims depending therefrom. Thus, Applicants respectfully request reconsideration and withdrawal of the § 103 rejection.

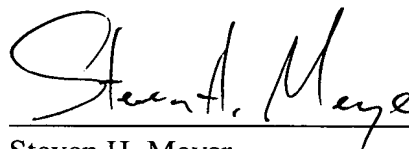
DOCKET NO.: MSFT-0135/147325.1
Application No.: 09/525,510
Office Action Dated: April 26, 2005

PATENT

In view of the foregoing discussion, Applicants respectfully submit that the present application, including claims 1-9, 11-14, 16-32, 34-37, and 39-46, is in condition for allowance, and such action is respectfully requested.

Respectfully Submitted

Date: July 6, 2005

A handwritten signature in cursive script, reading "Steven H. Meyer", written over a horizontal line.

Steven H. Meyer
Registration No. 37,189

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439